UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,813	02/09/2004	Shlomo Ovadia	42P18636	9229

45209 7590 03/18/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
03/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,813	OVADIA ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-27* is/are pending in the application.

4a) Of the above claim(s) *1-18* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the communication filed on 01/14/2009.

Claims 28-38 have been cancelled.

Claims 19 have been amended.

Claims 1-18 have been withdrawn from consideration.

Claims 19-27 have been examined and are pending.

Response to Arguments

Applicant's arguments filed 01/14/2009 have been fully considered but they are not persuasive.

The Applicant argues the following:

(A) "Applicants respectfully submit that the combination of Qiao, Biggs, Townsend, Stringer, and McMillan either alone or in combination, fails to disclose, teach, or suggest using a control burst (which are used to reserve network resources to form virtual lightpaths) to indicate whether or not a data burst will be encrypted."

The Examiner respectfully disagrees with the Applicant for the following reasons:

Per (A):

Qiao teaches generating a control burst, the control burst containing information to reserve network resources to form a virtual lightpath between the source edge node and the destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath segment **[Qiao: fig. 1b; pg. 105, Col. 1, 2nd paragraph; "In addition, by sending a**

control packet carrying routing information on a separate control wavelength (channel) and using an offset time (i.e. a lead time) before the transmission of the corresponding burst or data, FDL requirements can be eliminated as illustrated in Fig. 1b"; a control packet is equivalent to control burst. A wavelength is equivalent to lightpath. Burst or Data is equivalent to data burst].

adding information to the control burst [[indicating whether or not]] one or more data bursts to be sent from the source edge0 node to the destination edge node will be encrypted **[Qiao: fig. 1b; pg. 105, Col. 1, 2nd paragraph; "In addition, by sending a control packet carrying routing information on a separate control wavelength (channel) and using an offset time (i.e. a lead time) before the transmission of the corresponding burst or data, FDL requirements can be eliminated as illustrated in Fig. 1b"; a control packet is equivalent to control burst. A wavelength is equivalent to lightpath. Burst or Data is equivalent to data burst. Control packet processing setup/bandwidth reservation (see fig 1b)]**.

Qiao does not explicitly teach indicating whether or not one or more data bursts containing the data that are encrypted.

However, Biggs teaches indicating whether or not one or more data bursts containing the data that are encrypted **[Biggs: figs 2-5; par. [0014]; "a first indicator to indicate whether end-to-end encryption is applied to at least a portion of the payload and a second indicator to indicate whether air interface encryption is applied to at least a portion of the payload in each over-the-air"; See also [0018-0020].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao by including the step of Biggs of an Ethernet to provide users with a means for indicating and processing multiple levels of encryption to enhance a security **[Biggs: par. [0005].**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Chunming Qiao**, Optical Networking Solutions for next-generation Internet networks, "Label Optical Burst Switching for IP-over-WDM Integration", IEEE Communication Magazine, September 2000, pg.104-114 in view of **Biggs** et al. (US 2004/0236946 A1).

As per claim 19:

Qiao teaches a tangible machine-readable medium to provide instructions, which when executed by a processor in a source edge node of an optical switched (OS) network cause the source edge node to perform operations including:

generating a control burst, the control burst containing information to reserve network resources to form a virtual lightpath between the source edge node and the destination edge node

during a scheduled timeslot, the virtual lightpath including at least one lightpath segment **[Qiao: fig. 1b; pg. 105, Col. 1, 2nd paragraph; "In addition, by sending a control packet carrying routing information on a separate control wavelength (channel) and using an offset time (i.e. a lead time) before the transmission of the corresponding burst or data, FDL requirements can be eliminated as illustrated in Fig. 1b"; a control packet is equivalent to control burst. A wavelength is equivalent to lightpath. Burst or Data is equivalent to data burst]**

adding information to the control burst [[indicating whether or not]] one or more data bursts to be sent from the source edge0 node to the destination edge node will be encrypted **[Qiao: fig. 1b; pg. 105, Col. 1, 2nd paragraph; "In addition, by sending a control packet carrying routing information on a separate control wavelength (channel) and using an offset time (i.e. a lead time) before the transmission of the corresponding burst or data, FDL requirements can be eliminated as illustrated in Fig. 1b"; a control packet is equivalent to control burst. A wavelength is equivalent to lightpath. Burst or Data is equivalent to data burst. Control packet processing setup/bandwidth reservation (see fig 1b)]**;

sending the control burst to a first hop along the virtual lightpath, the first hop comprising one of a switching node or the destination edge node [**Qiao: pg. 107; Col. 1; 4th paragraph; "As shown in Fig. 2a, S sends out a control packet (i.e. control burst) to reserve bandwidth at each hop which is followed by a burst after an offset time T"; pg. 106, Col. 1, 6th paragraph; " In burst switching, a burst will cut through intermediate node (or switches)**

without being buffered, whereas in packet switching, a packet is stored and forwarded at each intermediate node (resulting in increased nodal complexity"]; and

sending said one or more data bursts containing the data to the first hop along the virtual lightpath during the scheduled timeslot **[Qiao: fig. 1b; pg. 105, Col. 1, 2nd paragraph; "In addition, by sending a control packet carrying routing information on a separate control wavelength (channel) and using an offset time (i.e. a lead time) before the transmission of the corresponding burst or data, FDL requirements can be eliminated as illustrated in Fig. 1b"; a control packet is equivalent to control burst. A wavelength is equivalent to lightpath. Burst or Data is equivalent to data burst. Control packet processing setup/bandwidth reservation (see fig 1b)]**.

Qiao does not explicitly teach indicating whether or not one or more data bursts containing the data that are encrypted.

However, Biggs teaches indicating whether or not one or more data bursts containing the data that are encrypted **[Biggs: figs 2-5; par. [0014]; "a first indicator to indicate whether end-to-end encryption is applied to at least a portion of the payload and a second indicator to indicate whether air interface encryption is applied to at least a portion of the payload in each over-the-air"; See also [0018-0020].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao by including the step of Biggs of an Ethernet to provide users with a means for indicating and processing multiple levels of encryption to enhance a security **[Biggs: par. [0005].**

Claims 20-21 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chunming Qiao**, Optical Networking Solutions for next-generation Internet networks, "Label Optical Burst Switching for IP-over-WDM Integration", IEEE Communication Magazine, September 2000, pg.104-114 in view of **Biggs** et al. (US 2004/0236946 A1) and further in view of **Townsend et al.** (US Patent 5,850,441).

As per claim 20:

Qiao and Biggs do not explicitly teach a tangible machine-readable medium wherein execution of the instructions further perform the operation of sending an encryption key to each of a plurality of edge nodes.

However, Townsend teaches a tangible machine-readable medium wherein execution of the instructions further perform the operation of sending an encryption key to each of a plurality of edge nodes in the OS network **[Townsend: Col. 8, lines 56-59, "The use of a multiple-access network and the establishing of different keys at different receivers on the network is described in further detail in the above cited International application file this day"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao and Biggs of by including the step of Townsend because it would to provide a fresh key may be transmitted periodically, to maintain security **[Townsend, Col. 8, lines 54-55].**

As per claim 21:

Qiao and Biggs teach the tangible machine-readable wherein execution of the instructions performs the operation of sending the encryption key to an edge node by:

generating a control burst containing security data including the encryption key or data from which the encryption key can be derived as described as claim 20 above.

Qiao and Biggs do not explicitly teach sending the control burst to a first hop along a virtual lightpath coupling the edge node sending the control burst to an edge node receiving the control burst, the first hop comprising one of the edge node receiving the control burst or a switching node.

However, Townsend teaches sending the control burst to a first hop along a virtual lightpath coupling the edge node sending the control burst to and edge node receiving the control burst, the first hop comprising one of the edge node receiving the control burst or a switching node **[Townsend: fig. 2, box 22 and 23].** Motivation is the same as claim 20.

As per claim 25:

Townsend further teaches the tangible machine-readable medium wherein an encryption key is sent to an edge node via a communication channel that is external from the OS network **[Townsend: Col. 5, lines 58-59; "The quantum key distribution channel is arranged to operate independently of other transmission channels which use the network to carry either the encrypted data or standard (non-encrypted) signals"].**

As per claim 26:

Qiao and Biggs do not explicitly teach a tangible machine-readable medium wherein execution

Instructions performs further operations including:

generating an encryption key, the encryption key to be used to encrypt the data; and

generating a decryption key corresponding to the encryption key**.**

However, Townsend teaches the tangible machine-readable medium wherein execution of the instructions performs further operations including:

generating an encryption key, the encryption key to be used to encrypt the data **[Townsend: Col. 5, lines 58-59; "The quantum key distribution channel is arranged to operate independently of other transmission channels which use the network to carry either the encrypted data or standard (non-encrypted) signals"; Col. 8, lines]**; and

generating a decryption key corresponding to the encryption key **[Col. 5, lines 58-59; "The quantum key distribution channel is arranged to operate independently of other transmission channels which use the network to carry either the encrypted data or standard (non-encrypted) signals"; Col. 1, lines 43-44; " as a key for encryption/decryption of subsequence data transmission between the two users of the channel"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao and Biggs of by including the step of Townsend because it would to provide a fresh key may be transmitted periodically, to maintain security **[Townsend, Col. 8, lines 54-55].**

Claims 22-23 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chunming Qiao**, Optical Networking Solutions for next-generation Internet networks, "Label

Optical Burst Switching for IP-over-WDM Integration", IEEE Communication Magazine, September 2000, pg.104-114 in view of **Biggs** et al. (US 2004/0236946 A1) further in view of **Townsend et al.** (US Patent 5,850,441) and further in view of **Stringer et al.** (US 2003/0196087 A1).

As per claim 22:

Qiao, Biggs, and Townsend do not explicitly teach the tangible machine-readable medium wherein the security data include a digital certificate.

However, Stringer teaches the tangible machine-readable medium wherein the security data include a digital certificate **[Stringer: par. [0021], lines 8-14; "Finally, it will be clear to one skilled in the art that as the document server recognizes entities to trust based on their keys, rather than who signed their digital certificates, and that arbitrary certificates, such as self-signed certificates (i.e., where the party to which the key pair belongs acts as its own certificate authority), or even unsigned public keys in isolation, may alternatively be used"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao, Biggs, and Townsend by including the step of Stringer because it would allow a party to which the key pair belongs acts as its own certificate authority **[Stringer, par. [0021], lines 12-13].**

As per claim 23:

Claim 23 is rejected with the same reason in claim 22 as described above.

As per claim 27:

Qiao, Biggs and Townsend do not explicitly teach the tangible machine-readable wherein execution of the instructions performs further operations including: " generating security data including the decryption key and identifying the decryption key as a public key, the security data comprising data from which an digital certificate may be issued; and sending the security data to a certificate authority".

However, Stringer teaches,

generating security data including the decryption key and identifying the decryption key as a public key, the security data comprising data from which an digital certificate may be issued **[Stringer: par. [0018]; "The operating environment 100 also includes a public key infrastructure (PKI). In the PKI, typically a certificate authority 118 or a trusted third party is used to sign digital certificates 120, 132, and 134 issued to the document server 102, user A of the device 106, and user B of the device 108, respectively. The public key infrastructure permits two parties to dynamically establish secure communications with each other without ever having a prior relationship through the use of a digital certificate"]**; and

sending the security data to a certificate authority **[Stringer: par. [0018]; par. [0021], lines 1-8].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the step of Qiao, Biggs, and Towsend of the invention each public key is included as part of a digital certificate that is held by each part (e.g., the first user,

the second user, or the document server) holding the private key associated with that certificates **[Stringer, par. [0008]].**

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Chunming Qiao**, Optical Networking Solutions for next-generation Internet networks, "Label Optical Burst Switching for IP-over-WDM Integration", IEEE Communication Magazine, September 2000, pg.104-114 in view of **Biggs** et al. (US 2004/0236946 A1) further in view of **Townsend et al.** (US Patent 5,850,441) and further in view of **McMillan et al.** (US 2004/0039925 A1).

As per claim 24:

Qiao, Biggs, and Townsend do not explicitly teach a tangible machine-readable medium wherein the security data include one of information identifying an encryption algorithm used to encrypt the data or executable code that may be used to decrypt the certificate.

However, McMillan teaches a tangible machine-readable medium wherein the security data include one of information identifying an encryption algorithm used to encrypt the data or executable code that may be used to decrypt the certificate **[McMillan: fig. 8A; par. [0027]; "The message 600 additionally includes a signature 606 generated by the user. To generate the signature 606, the user generates a message digest, or hash, 608 using a standard algorithm such as, for example, the Secure Hashing algorithm SHA-1, using the header 602 and any data 604 as input to the algorithm"].**

Therefore, it would have been obvious to apply a known technique to a known device ready for improvement to yield predictable results by using the same algorithm at a receiver end.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zand Kambiz can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

March 13, 2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434